Division of Information Security
Protecting our information systems

System Security Certification and Accreditation (C&A) Framework

Dave Dickinson, IOAT ISSO
Chris Tillison, RPMS ISSO

Indian Health Service
5300 Homestead Road, NE
Albuquerque, NM 87110
(505) 248-4500
fax: (505) 248-4115

Overview

- Security Certification
- Security Accreditation
- Terminology
- Managing Enterprise Risk
  - Security Categorization
  - Security Control Selection
  - Security Control Refinement
  - Security Control Documentation
  - Security Control Implementation
  - Security Control Assessment
  - System Authorization
  - Security Control Monitoring
- The C&A Process
- Basic C&A Documents

Question?

What is Certification?

Security Certification

- The comprehensive evaluation of the management, operational, and technical security controls in an information system
- Evaluation supports the security accreditation process
- Evaluation performed by security expert (may be contractor)
- Assesses the effectiveness of the implemented security controls in a particular environment of operation
  - Are the controls an acceptable set?
  - Are the controls operating as intended?
- Determines remaining vulnerabilities in the information system based on the assessment.

Question?

What is Accreditation?

Security Accreditation

- The official management decision to authorize operation of an IT system
  - Residual risk is one factor in decision
- Authorization:
  - Is given by a senior agency official (RPMS Designated Accrediting Authority (DAA) is Phyllis Eddy)
  - Is applicable to a particular environment of operation of the IT system
  - Explicitly accepts the level of residual risk to agency operations (including mission, functions, image or reputation), assets, & individuals that remain after the implementation of an agreed upon set of security controls in the IT system.

Terminology

- Security certification: Assessing/verifying effectiveness of implemented security controls
- Security accreditation: Approval/authorization to operate IT system

Managing Enterprise Risk

The Framework

Starting Point

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

FIPS 200 / SP 800-53

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-37

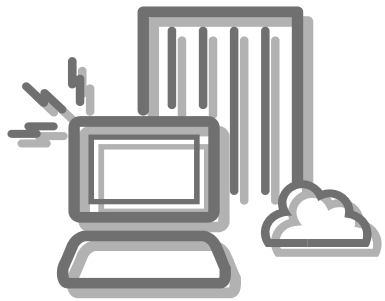
Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements



SP 800-37

System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-18

Security Control Documentation

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Security Categorization Information

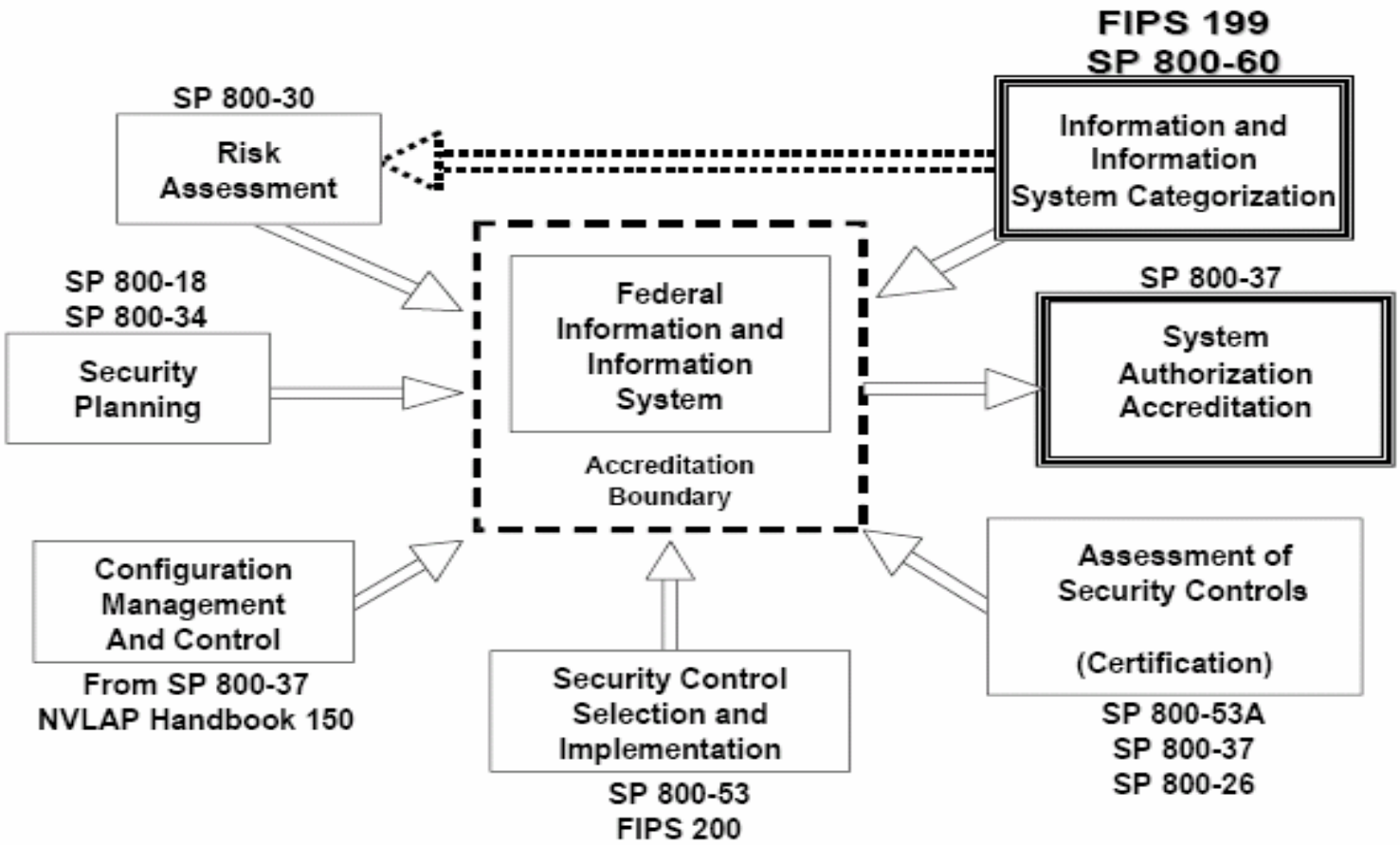


Figure 2: FIPS 199 and SP 800-60 Role in Information Security Program

Security Categorization Information

FIPS 199 ***(Standards for Security Categorization of Federal Information and Information Systems)***
SP 800-60 (***Guide for Mapping Types of Information and Information Systems to Security Categories***)

- Security Objectives:
  - Confidentiality
  - Integrity
  - Availability
- Levels of Impact:
  - Low = **Limited** adverse effect on organizational operations
  - Moderate = **Serious** adverse effect on organizational operation
  - High = **Severe** or catastrophic adverse effect on organizational operations
- Security Category = {(confidentiality, impact), (integrity, impact), (availability, impact)}

Security Categorization Cont.

Guidance for Mapping Types of Information and Information Systems to FIPS Publication 199 Security Categories

SP 800-60

FIPS Publication 199	Low	Moderate	High
Confidentiality	The loss of confidentiality could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of confidentiality could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The loss of integrity could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of integrity could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The loss of availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The loss of availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Example: An Enterprise Information System

Security Categorization Cont.

- EXAMPLE 1: IHS RPMS Information System Impact Levels and Categorization

Step 1: Review Information System Provisional Impact Levels												
Security Category (Info System)	=	{(	Confidentiality,	MODERATE	),(	Integrity,	HIGH	),(	Availablity,	MODERATE	)}
Step 2: Adjust Information System Impact Levels												
Security Category (Info System)	=	{(	Confidentiality,	HIGH	),(	Integrity,	HIGH	),(	Availablity,	MODERATE	)}
Step 3: Finalized Information System Impact Levels												
Security Category (Info System)	=	{(	Confidentiality,	HIGH	),(	Integrity,	HIGH	),(	Availablity,	MODERATE	)}

- IHS RPMS Security Categorization is rated (HIGH)

Step 3: Finalized Information System Impact Levels (IOAT) System												
Security Category (Info System)	=	{(	Confidentiality,	HIGH	),(	Integrity,	HIGH	),(	Availablity,	MODERATE	)}
Step 3: Finalized Information System Impact Levels (NPIRS) System												
Security Category (Info System)	=	{(	Confidentiality,	MODERATE	),(	Integrity,	LOW	),(	Availablity,	LOW	)}

- IHS IOAT & NPIRS Security Categorization

Security Control Selection

- Management Controls
  - Risk Assessment (RA)
    - (RA-2) Security Categorization L, M, H
  - Planning (PL)
    - (PL-2) System Security Plan L, M, H
  - System and Service Acquisition (SA)
    - (SA-7) User Installed Software L, M, H
  - Certification, Accreditation, and Security Assessments (CA)
    - (CA-5) Plan of Action and Milestones - L, M, H

Security Control Selection

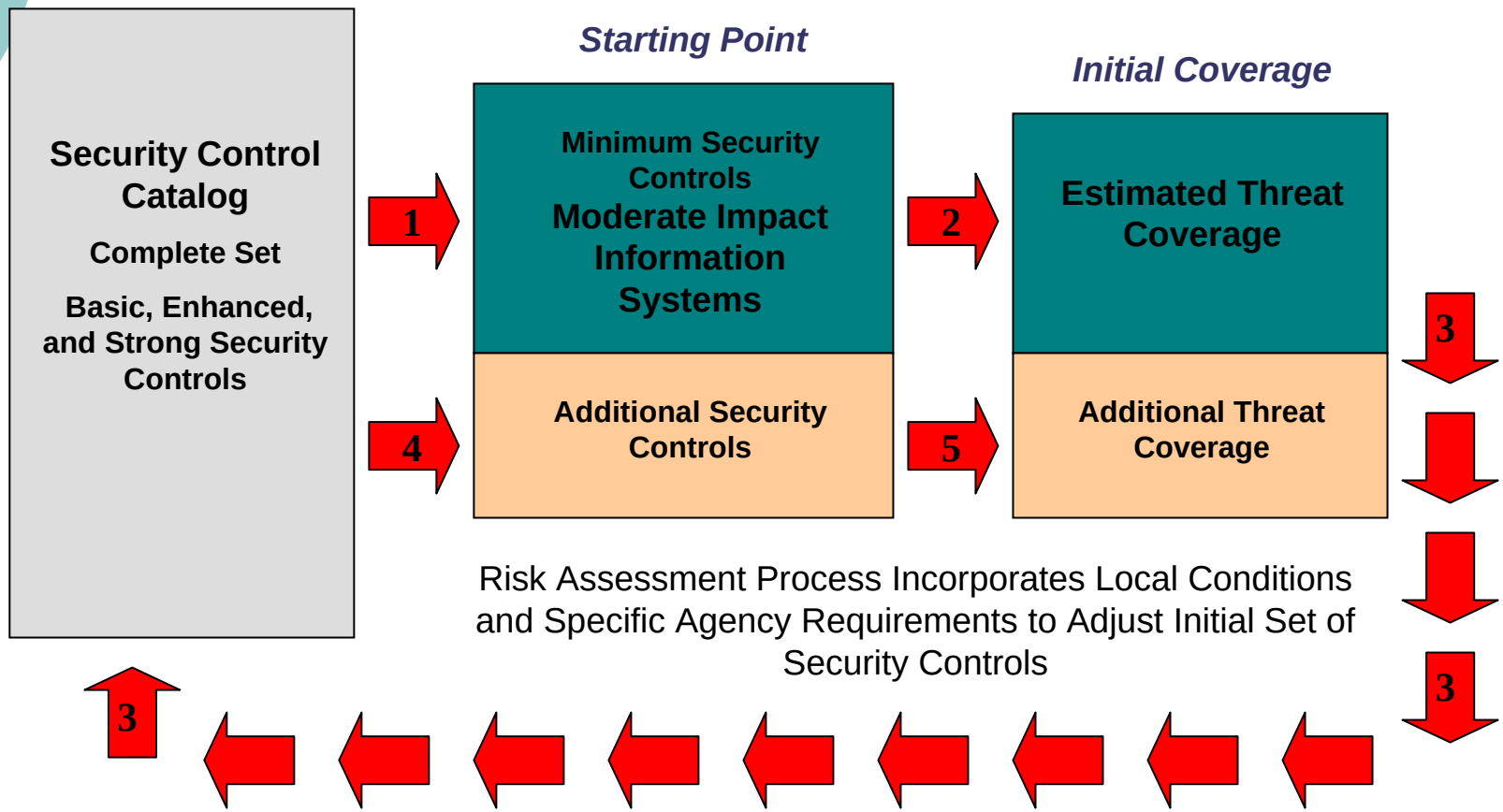
- Operational Controls
  - Personnel Security (PS)
    - (PS-3) Personnel Screening L, M, H
  - Physical and Environmental Protection (PE)
    - (PE-17) Alternate Worksite M, H
  - Contingency Planning (CP)
    - (CP-3) Contingency Training M, H(1)
  - Configuration Management (CM)
    - (CM-7) Least Functionality M, H(1)
  - Maintenance (MA)
    - (MA-6) Timely Maintenance M, H
  - System and Information Integrity (SI)
    - (SI-8) Spam and Spyware Protection M, H
  - Media Protection (MP)
    - (MP-5) Media Transport M, H
  - Incident Response (IR)
    - (IR-6) Incident Reporting L, M, H
  - Awareness and Training (AT)
    - (AT-3) Security Training - L, M, H

Security Control Selection

- Technical Controls
  - Identification and Authentication (IA)
    - (IA-6) Authentication Feedback L, M, H
  - Access Control (AC)
    - (AC-9) Previous Logon Notification – Not Selected
  - Audit and Accountability (AU)
    - (AU-8) Time Stamps M, H
  - System and Communications Protection (SC)
    - (SC-14) Public Access Protections L, M, H

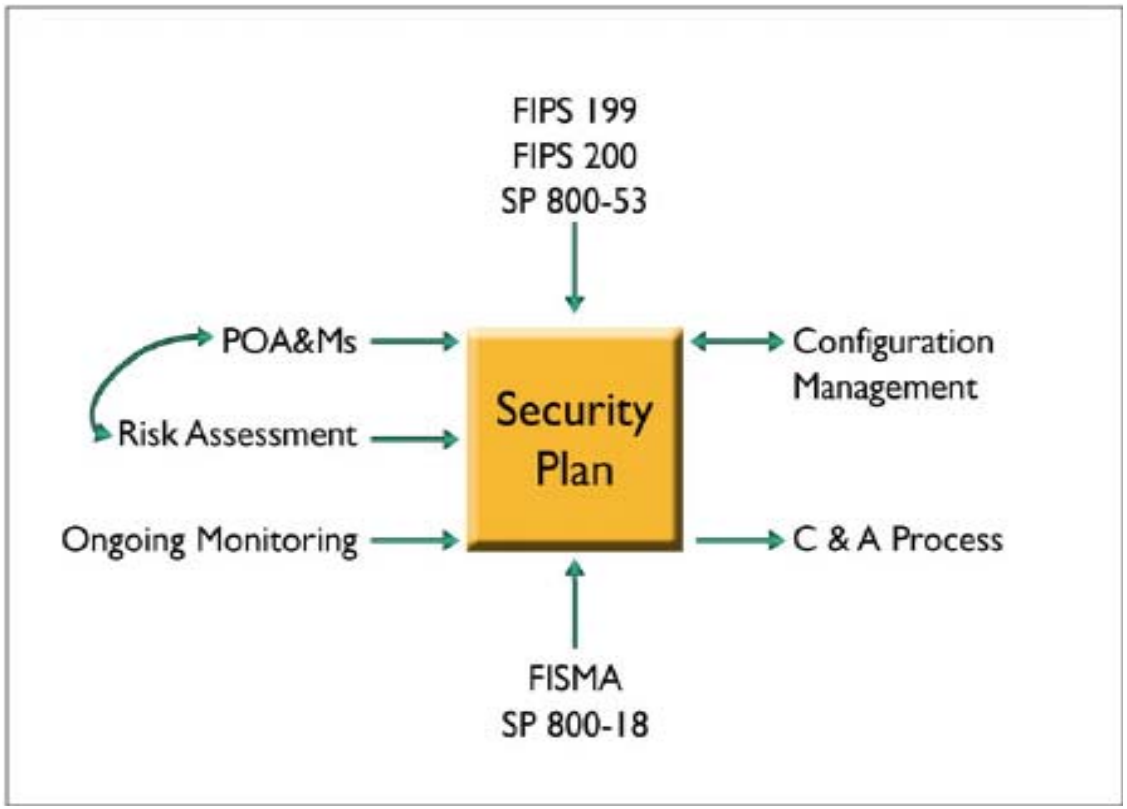
Security Control Refinement

- **FIPS 200** ***(Minimum Security Requirements for Federal Information and Information Systems)***
- **NIST SP 800-30** ***(Risk Management Guide for Information Technology Systems)***
- **NIST SP 800-53** ***(Recommended Security Controls for Federal Information System)***



Security Control Documentation

- **NIST 800-18** ***(Guide for Developing Security Plans for Federal Information Systems)***



Security Control Documentation

- Security Plan
- Risk Assessment
- Contingency Plan
- System Specifications
- Architecture and Design
- User Manuals
- Operating Procedures
- Network Diagrams
- Configuration Mgmt.

Security Control Documentation

- Management Controls
  - (CA-5) Plan of Action and Milestones - L, M, H

    This is an enterprise common security control.

    Ref: NIST 800-65 “Integrating IT Security into the Capital Planning and Investment Control Process

    HHS Plan of Actions and Milestone Guide July 19, 2005

    HHS Certification and Accreditation Guide

    HHS Information Security Program Handbook 01 December 2005

    IHS OIT Certification and Accreditation Guide (SOP 05-15)

    In Place Controls: Plan of actions and milestones (POA&Ms) are submitted into the HHS portfolio management software for the RPMS. POA&M’s are maintained continuously and a quarterly status report is generated.

Security Control Documentation

- Operational Controls
  - (AT-3) Security Training - L, M, H

    Ref: HHS Information Security Program Policy 19 July 2005

    HHS IT Security Handbook 01 December 2005

    IHS Providing Security Training (SOP 05-38)

    In Place Controls: Staff that has information security duties as a major portion of their position will receive additional training annually. The training will be documented in the employees file and with the supervisor.

Security Control Documentation

- Technical Controls
  - (AC-9) Previous Logon Notification

    Ref: Kernel Systems Manual v8.0 July 1995

    In Place Control: RPMS displays previous login date and time as well as login failures.

Security Control Implementation

- **SP 800-70** ***(Security Configuration Checklist for IT Products – Guidance for Checklist Users and Developers)***

A *security configuration checklist* is sometimes referred to as a lockdown guide, hardening guide, security guide, or a security technical implementation guide. You may find a list of NIST Provided Checklist's at http://checklists.nist.gov/repository/index.html.

Product Categories:

- Application Servers
- Antivirus Software
- Database Systems
- DNS Servers
- Firewalls…

Security Control Assessment

- **NIST SP 800-37** ***(Guide for the Security Certification and Accreditation of Federal Information Systems)***
- **NIST SP 800-26** ***(*****Guide for Information Security Program Assessments and System Reporting Form*****)***
- **NIST SP 800-53A** **(Guide for Assessing the Security Controls in Federal Information Systems)**

- **Security Testing and Evaluation, Self Assessment, Risk Assessment**
  - Documenting and supporting materials
  - Reuse of assessment results
  - Methods and procedures
  - Security assessment
  - Security assessment report
  - Evaluate the security controls – may include penetration testing

System Authorization

- **NIST SP 800-37** ***(Guide for the Security Certification and Accreditation of Federal Information Systems)***

- Authorization to Operate

The authorizing official deems that the risk to agency operations, agency assets, or individuals is acceptable, acceptable, an authorization to operate is issued for the information system.

- Interim Authorization to Operate

The authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation, an interim authorization to operate may be issued.

- Denial of Authorization to Operate

The authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, the authorization to operate the information system is denied.

Security Control Monitoring

- **NIST SP 800-37** ***(Guide for the Security Certification and Accreditation of Federal Information Systems)***

3 Tasks of Security Monitoring:

1) Configuration Management and Control
   a) Track changes to the information system
2) Security Control Monitoring
   a) Analyze the security impact of those changes
3) Status Report and Documentation
   a) Make appropriate adjustments to the security controls and the System Security Plan

Basic C&A Documents

- System Security Plan
  - Provide an overview of security requirements for the IT system and describe planned security controls (management, operational and technical).
- Risk Assessment Report
  - Documents the results of risk assessment activities, threats, vulnerabilities, control effectiveness and trade-offs (performance impact and cost).
- Security Test and Evaluation Reports
  - Document the results of verifying compliance to security requirements and that security controls are correctly implemented and effective.
- Certifier's Statement
  - Overview of security status.

SUMMARY

- Develop a System Security Plan (SSP)
- Have a Risk Assessment (RA) performed
- System Test & Evaluation (Annually)
- Continuous Monitoring

Questions?

Dave Dickinson, IOAT ISSO

David.Dickinson@ihs.gov

Chris Tillison, RPMS ISSO

Chris.Tillison@ihs.gov

Indian Health Service
5300 Homestead Road, NE
Albuquerque, NM 87110
(505) 248-4500
fax: (505) 248-4115